

WHAT IS CLAIMED IS:

- Sub
C2
- 1 1. A method for encoding transaction data, the transaction data including account
2 PIN data and non-PIN data, comprising the steps:
3 performing a first encryption operation only on the PIN data; and
4 performing a second encryption operation on at least the non-PIN data, such that
5 the PIN data is cryptographically isolated from the non-PIN data.
 - 1 2. The method of encoding transaction data of claim 1, wherein:
2 said first encryption operation uses an asymmetrical encryption process; and
3 said second encryption operation uses a symmetrical encryption process.
 - 1 3. The method of encoding transaction data of claim 2, wherein said symmetrical
2 encryption process uses a secret encryption key and wherein said method includes the
3 further step of performing a third encryption operation on said secret encryption key.
 - 1 4. The method of encoding transaction data of claim 1, wherein said second
2 encryption process is performed on both the PIN and non-PIN data, such that the
3 encrypted PIN data resides within an encrypted envelope generated by the second
4 encryption operation.
 - 1 5. The method of encoding transaction data of claim 1, further comprising the steps of:

2 calculating a digest by applying a one-way mathematical process to the non-PIN
3 data; and
4 appending the digest to the PIN data blocks for future verification of the non-PIN
5 data.

1 6. A method for decoding encrypted transaction data, the transaction data including
2 account PIN data as well as non-PIN data, comprising the steps:

3 performing a first decryption operation to decode the non-PIN data; and
4 performing a second decryption operation to decode the PIN data, wherein said
5 second decryption operation is different from the first decryption operation.

1 7. The method of decoding encrypted transaction data of claim 6, wherein:
2 said first decryption operation uses a symmetrical decryption process; and
3 said second decryption operation uses an asymmetrical decryption process.

1 8. The method of decoding encrypted transaction data of claim 6, further comprising
2 the steps:

3 calculating a digest by applying a one-way mathematical process to the non-PIN
4 data; and

5 comparing the calculated digest to a received digest formed with the same one-
6 way mathematical process and appended to the PIN data blocks for verifying the non-PIN
7 data.

1 9. A method for encoding account related data comprising the steps:
2 analyzing the account related data to identify PIN-related data blocks and non-
3 PIN data blocks;
4 performing a first encryption operation only on said PIN-related data blocks; and
5 performing a second encryption operation on at least said non-PIN data blocks.

1 10. The method for encoding account related data of claim 9, wherein:
2 said first encryption operation uses an asymmetrical encryption process; and
3 said second encryption operation uses a symmetrical encryption process.

1 11. The method for encoding account related data of claim 10, wherein said
2 symmetrical encryption process uses a secret encryption key and wherein said method
3 includes the further step of performing a third encryption operation on said secret
4 encryption key.

1 12. The method for encoding account related data of claim 10, wherein said second
2 encryption operation is performed on both the PIN and non-PIN data, such that the
3 encrypted PIN data resides within an encrypted envelope generated by the second
encryption operation.

1 13. The method of encoding account related data of claim 9, further comprising the
2 steps of:

1 calculating a digest by applying a one-way mathematical process to the non-PIN
2 data; and
3 appending the digest to the PIN data blocks to allow for future verification of the
4 non-PIN data.

1 14. The method of encoding account data of claim 9, wherein the account data is
2 associated with a payment instrument selected from the group including a credit card, a
3 debit card and a "smart" card.

1 15. A method of transporting PIN and non-PIN data in a secure electronic transfer,
2 comprising the steps:
3 encrypting only the PIN data using a first encryption process,
4 encrypting at least the non-PIN data using a second encryption process;
5 transmitting the encrypted PIN and non-PIN data to an authentication requestor,
6 said authentication requestor having means to decrypt only the non-PIN data;
7 transmitting the encrypted PIN data to an authorizing agent for verification;
8 decrypting and verifying the PIN data by the authorizing agent; and
9 transmitting a notification, from the authorizing agent to the authentication
10 requestor, of a verification status of the PIN data.

1 16. The method of transporting PIN and non-PIN data of claim 15, wherein said
2 second encryption process is different from the first encryption process;

1 17. The method of transporting PIN and non-PIN data of claim 16, wherein:
2 said first encryption process is an asymmetrical encryption process; and
3 said second encryption process is a symmetrical encryption process.

1 18. The method of transporting PIN and non-PIN data of claim 17, wherein the
2 asymmetrical encryption process is performed using a public key provided to an account
3 holder by the authorizing agent and wherein said decrypting performed by the authorizing
4 agent is performed using a private key associated with the public key.

1 19. The method of transporting PIN and non-PIN data of claim 18, wherein said
2 symmetrical encryption process uses a secret encryption key and wherein said method
3 includes the further step of performing a third encryption operation on said secret
4 encryption key.

1 20. The method of transporting PIN and non-PIN data of claim 16, further comprising
2 the steps of:
3 prior to transmitting the encrypted PIN and non-PIN data, calculating a first digest
4 by applying a one-way mathematical process to the non-PIN data and appending the
5 digest to the PIN data blocks; and
6 after transmitting the encrypted PIN and non-PIN data, calculating a second digest
7 by applying the same one-way mathematical process to the non-PIN data and comparing
8 the first digest and second digest to verify the non-PIN data.

1 21. A terminal for encoding transaction data including account PIN data as well as
2 non-PIN data, comprising:

3 means for performing a first encryption operation only on the PIN data; and

4 means for performing a second encryption operation on at least the non-PIN data,

5 such that the PIN data is cryptographically isolated from the non-PIN data.

1 22. The terminal for encoding transaction data of claim 21, wherein:

2 said first encryption means uses an asymmetrical encryption process; and

3 said second encryption means uses a symmetrical encryption process.

1 23. The terminal for encoding transaction data of claim 21, further comprising a card
2 reader for acquiring at least a portion of the transaction data from a payment instrument.

1 24. A system for decoding encrypted transaction data including account PIN data as
2 well as non-PIN data, comprising:

3 means for performing a first decryption operation to decode the non-PIN data; and

4 means for performing a second decryption operation to decode the PIN data,

5 wherein said second decryption operation is different from the first decryption operation.

1 25. The system as defined by claim 24, wherein:

2 said first decryption means uses a symmetrical decryption process; and

3 said second decryption means uses an asymmetrical decryption process.

1 26. A system for encoding and transporting PIN and non-PIN data comprising:
2 first means for encrypting only the PIN data using a first encryption process;
3 second means for encrypting at least the non-PIN data using a second encryption
4 process;
5 means for transmitting the encrypted PIN and non-PIN data to an authentication
6 requestor, said authentication requestor having means to decrypt only the non-PIN data;
7 means for transmitting the encrypted PIN data to an authorizing agent for
8 verification;
9 means for decrypting and verifying the PIN data by the authorizing agent; and
10 means for notifying the authentication requestor of a verification status of the PIN
11 data.

1 27. The system for encoding and transporting PIN and non-PIN data of claim 26,
2 wherein said second encryption process is different from the first encryption process

1 28. The system for encoding and transporting PIN and non-PIN data of claim 27,
2 wherein:
3 said first encryption means employs an asymmetrical encryption process; and
4 said second encryption means employs a symmetrical encryption process.

1 29. The system for encoding and transporting PIN and non-PIN data of claim 27,
2 wherein the first encryption means uses a public key provided to an account holder by the

3 authorizing agent and wherein said decrypting means uses a private key associated with
4 the public key.

1 30. The system for encoding and transporting PIN and non-PIN data of claim 26,
2 further comprising:

3 means for calculating a first digest by applying a one-way mathematical process
4 to the non-PIN data and appending the digest to the PIN data blocks prior to transmitting
5 the encrypted PIN and non-PIN data; and

6 means for calculating a second digest by applying the same one-way
7 mathematical process to the non-PIN data and comparing the first digest and second
8 digest after transmitting the encrypted PIN and non-PIN data, to verify the non-PIN data.

1 31. The system for encoding and transporting PIN and non-PIN data of claim 24,
2 further comprising a card reader for acquiring at least a portion of the PIN and non-PIN
3 data from a payment instrument.